

TOP WINDOWS 2000 VULNERABILITIES

We're Sorry for the Inconvenience...





Default Installations

- IIS loads by Default!
- MANY potentially dangerous services are enabled by default.
- Many ports allowing unnecessary services.



Weak Passwords

- SQL server has SA password – often blank.
- Password same as account name.
- Easy to guess.
- Shared with co-workers.



Physical Access

- Server in open access area.
- Servers in offices.
- Too many people have access to server area.



SNMP Strings

- Simple Network Management Protocol.
- Default string is always public.
- Data Enumeration –
 user accounts, interfaces
 and much more.



NetBIOS Null Session

- AKA Anonymous Logon
- Allows connecting to a network without authentication.
- Allows anonymous enumeration of system information – usernames, share names, etc.



File Sharing

- May allow sensitive files to be shared. With Everyone.
- May allow others to run processes on your machine.
- Very dangerous when combined with null sessions.



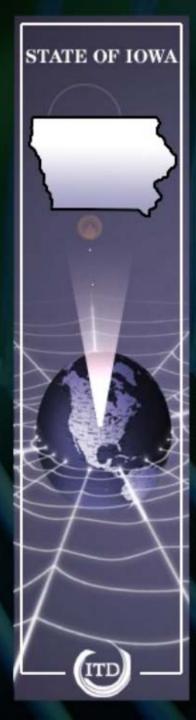
Disabling Null Sessions

- To disable both Null Sessions and File sharing, Ports 139 and 445, simply disable file and print sharing.
- To decrease the risk of allowing file sharing, set the RestrictAnonymous key.



Applications on OS Partition

• Applications, including IIS, should not be installed on the same partition as the operating system, which is the default in a standard installation.



Admin-Equivalent Accounts

- Too many powerful accounts on a network.
- Follow the rule of least permissions.



Failure to Apply Patches.

- Unicode Vulnerability,
 Directory Traversal attack –
 used by Nimda.
- Unpatched workstations can allow a normal user to gain administrative access through local promotion bugs.



Patch Identification

 Visit this site to find listings of all post service pack patches and hot fixes that should be applied to your system:

http://www.microsoft.com/technet/treeview/default.asp?url=/tec hnet/security/current.asp



Failure to Patch continued:

 IDA Overflow vulnerability was Used by both versions of Code Red.



Useful Web Sites

- http://www.itd.state.ia.us/security/
- http://nsa1.www.conxion.com/win2k/download.htm
- http://nsa2.www.conxion.com/support/download.htm

Dangerous Services in Win 2K - What they are, functions, and why they are dangerous.

- www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16301
- <u>www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16363</u>
- <u>www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16476</u>

Microsoft Network Security Hotfix Checker (HFNetChk) v. 3.2

• www.microsoft.com/Downloads/Release.asp?ReleaseID=31154